

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
1 septembre 2005 (01.09.2005)

PCT

(10) Numéro de publication internationale
WO 2005/081452 A1

(51) Classification internationale des brevets⁷ : **H04L 9/32**

(21) Numéro de la demande internationale :
PCT/FR2005/000158

(22) Date de dépôt international :
24 janvier 2005 (24.01.2005)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0450129 23 janvier 2004 (23.01.2004) FR

(71) Déposants (pour tous les États désignés sauf US) :
FRANCE TELECOM [FR/FR]; 6, place d'Alleray,
F-75015 Paris (FR). **MATH RIZK** [BE/BE]; SPRL, Verte
Voie 20, Boîte 5, B-1348 Louvain-La-Neuve (BE).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : **GUILLOU,**
Louis [FR/FR]; 16, rue de l'Ise, F-35230 Bourgarre (FR).
QUISQUATER, Jean-Jacques [BE/BE]; 3, avenue des
Canards, B-1640 Rhode Saint-Genèse (BE).

(74) Mandataire : **MUSTAKI, Daniel**; France Telecom, Divi-
sion R & D/PIV/PI, 38-40 rue du Général Leclerc, F-92794
Issy Moulineaux Cedex 9 (FR).

(81) États désignés (sauf indication contraire, pour tout titre de
protection nationale disponible) : AE, AG, AL, AM, AT,
AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO,

CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB,
GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG,
KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG,
MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH,
PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés (sauf indication contraire, pour tout titre
de protection régionale disponible) : ARIPO (BW, GH,
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,
ZW), eurasién (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO,
SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN,
GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

- relative au droit du déposant de demander et d'obtenir un
brevet (règle 4.17.ii)) pour toutes les désignations
- relative au droit du déposant de revendiquer la priorité de
la demande antérieure (règle 4.17.iii)) pour toutes les dési-
gnations
- relative à la qualité d'inventeur (règle 4.17.iv)) pour US
seulement

Publiée :

- avec rapport de recherche internationale
- avant l'expiration du délai prévu pour la modification des
revendications, sera republiée si des modifications sont re-
çues

En ce qui concerne les codes à deux lettres et autres abrégia-
tions, se référer aux "Notes explicatives relatives aux codes et
abréviations" figurant au début de chaque numéro ordinaire de
la Gazette du PCT.

(54) Title: ZERO-KNOWLEDGE PROOF CRYPTOGRAPHY METHODS AND DEVICES

(54) Titre : PROCEDES ET DISPOSITIFS CRYPTOGRAPHIQUES SANS TRANSFERT DE CONNAISSANCE

(57) Abstract: A cryptography method using a key holder having a number $m = 1$ of private keys Q_1, Q_2, \dots, Q_m and respective public keys G_1, G_2, \dots, G_m , where each key pair (Q_i, G_i) (where $i = 1, \dots, m$) fits either the equation $G_i = Q_i^v \bmod n$, or the relation $G_i \times Q_i^v = 1 \bmod n$, where n is a public integer equal to the product of f private prime factors (where $f > 1$), denoted by p_1, \dots, p_f of which at least two are different, and exponent v is a public integer equal to a power of 2. In particular, the invention teaches the mathematical structure that can be imparted to the public keys in order to make it impossible to calculate said private keys (within a reasonable amount of time) on the basis of the public parameters, unless the prime factors are known. The invention further relates to various devices for carrying out the method.

(57) Abrégé : L'invention concerne un procédé de cryptographie mettant en jeu un détenteur de clés possédant un nombre $m \geq 1$ de clés privées Q_1, Q_2, \dots, Q_m et de clés publiques respectives G_1, G_2, \dots, G_m , chaque paire de clés (Q_i, G_i) (où $i = 1, \dots, m$) vérifiant soit la relation $G_i = Q_i^v \bmod n$, soit la relation $G_i \times Q_i^v = 1 \bmod n$, où n est un entier public égal au produit de f facteurs premiers privés (où $f > 1$), notés p_1, \dots, p_f , dont deux au moins sont distincts, et l'exposant v est un entier public égal à une puissance de 2. L'invention enseigne notamment quelle structure mathématique on peut donner aux clés publiques de manière à ce qu'il soit impossible, à partir desdits paramètres publics, de calculer (en un temps raisonnable) lesdites clés privées, à moins de connaître lesdits facteurs premiers. L'invention concerne également divers dispositifs destinés à mettre en œuvre ce procédé.



WO 2005/081452 A1

Procédés et dispositifs cryptographiques sans transfert de connaissance

La présente invention concerne la cryptographie à clés asymétriques (également appelée "cryptographie à clé publique"). Plus précisément, elle
5 concerne un procédé et un système servant à vérifier l'authenticité d'une entité connue ou d'un message provenant d'une entité connue, ou encore à signer un message.

On rappelle que les systèmes de cryptographie à clés asymétriques comprennent des détenteurs de paires de clés, chaque paire comprenant
10 une clé dite "publique" et une clé dite "privée" (chaque clé pouvant d'ailleurs comporter plusieurs paramètres). Chaque clé publique est liée à l'identité de son détenteur par une autorité de certification. Les systèmes de cryptographie à clés asymétriques comprennent également des entités appelées "contrôleurs", qui ont enregistré un certain nombre de clés
15 publiques conjointement avec les identités certifiées de leurs détenteurs.

Depuis l'invention du procédé cryptographique à clés asymétriques dit "RSA" (initiales des inventeurs R. Rivest, A. Shamir et L. Adleman, cf. l'article de M. Gardner intitulé "*A new kind of cipher that would take millions
20 of years to break*", Scientific American, août 1977), le problème de la factorisation des nombres entiers a fait l'objet d'intenses recherches. Malgré de notables progrès (résultant d'ailleurs davantage de l'évolution de la puissance des ordinateurs que de celle des algorithmes de factorisation), on ne connaît toujours pas de méthode permettant de factoriser un grand nombre entier en un temps raisonnable. C'est donc à juste titre que les
25 utilisateurs font confiance au procédé RSA.

Chaque mise en œuvre du procédé RSA est associée à un entier appelé "module", noté n , qui est le produit de deux grands facteurs premiers distincts p_1 et p_2 . Compte tenu des capacités de calcul actuelles, il est
30 conseillé d'utiliser des modules de 1024 bits (de l'ordre de 10^{308}) au moins. Une clé publique RSA comprend le module n , et un "exposant" e qui est premier avec $(p_1 - 1)$ et avec $(p_2 - 1)$. La clé privée RSA correspondante comprend un "exposant" d tel que :

$$e \times d = 1 \mod [(p_1 - 1)(p_2 - 1)]$$

(le symbole "mod" signifie "modulo"). La sécurité de ce procédé repose sur
35 le fait qu'il est impossible en un temps raisonnable de calculer d à partir de n et e si l'on ne connaît pas les facteurs p_1 et p_2 . Comme expliqué ci-dessus, il n'est pas possible de calculer ces facteurs (qui sont naturellement tenus secrets) en un temps raisonnable.

La procédure cryptographique dite "d'authentification d'entités" met
40 en présence un contrôleur et un détenteur de clés, appelé ici "démonstrateur", qui souhaite être authentifié par le contrôleur afin de recevoir une certaine autorisation, par exemple un droit d'accès à des ressources informatiques. Le démonstrateur déclare son identité au contrôleur et doit lui prouver qu'il détient bien la clé privée correspondant à la
45 clé publique liée à cette identité.

Il est possible de réaliser cette authentification sans que le démonstrateur ne divulgue la moindre information sur sa clé privée au contrôleur: on parle alors d'authentification "sans transfert de connaissance" (en anglais, "*zero-knowledge proof*"). Cette technique a été décrite dans sa
 5 généralité par S. Goldwasser, S. Micali et C. Rackoff dans leur communication au "17th ACM Symposium on the Theory of Computing" intitulée "*The Knowledge Complexity of Interactive Proof Systems*" (Actes pages 291 à 304, 1985).

Dans l'article intitulé "*Zero-knowledge Proofs of Identity*" (Journal of
 10 Cryptology, vol. 1, pages 77 à 94, 1988), U. Feige, A. Fiat et A. Shamir ont proposé un procédé cryptographique "sans transfert de connaissance", dans lequel le démonstrateur, d'une part, détient une clé privée Q , et d'autre part a publié un module RSA n ainsi qu'une clé publique $G = Q^2 \bmod n$ (le calcul de Q à partir de G , c'est-à-dire le calcul d'une racine carrée modulo n , est
 15 impossible en un temps raisonnable à moins que l'on ne connaisse les facteurs premiers de n).

En ce qui concerne l'application de ce procédé à l'authentification d'entités, la procédure dite de "Fiat-Shamir" comprend les étapes interactives suivantes:

- 20 1. *Etape d'engagement*: le démonstrateur choisit aléatoirement un entier r , calcule "l'engagement" $R = r^2 \bmod n$, et envoie l'engagement au contrôleur;
2. *Etape de défi*: le contrôleur choisit aléatoirement un entier d appelé "défi", qui peut prendre la valeur 0 ou la valeur 1, et envoie ce défi au
 25 démonstrateur;
3. *Etape de réponse*: le démonstrateur calcule la "réponse" $D = r \times Q^d \bmod n$, et envoie cette réponse au contrôleur; et
4. *Etape de vérification*: le contrôleur calcule $\left(\frac{D^2}{G^d} \right) \bmod n$, et vérifie que
 le résultat est bien égal à l'engagement R .

30 Il est de plus conseillé, pour une plus grande sécurité, de répéter toute cette procédure "en série" un nombre de fois aussi grand que possible (en faisant varier r et d à chaque fois) avant de considérer que l'authentification a bien été effectuée.

35 Il s'agit bien d'une procédure "sans transfert de connaissance", car un observateur ne peut, à partir des données échangées, calculer la clé privée Q du démonstrateur.

Selon une variante, dite de "Feige-Fiat-Shamir" ou "en parallèle", le démonstrateur détient un nombre $m > 1$ de clés privées Q_1, Q_2, \dots, Q_m , et a publié, outre un module RSA n , une pluralité de clés publiques respectives

G_1, G_2, \dots, G_m , où $G_i = Q_i^2 \bmod n$ pour $i = 1, \dots, m$. On met alors en œuvre les étapes suivantes:

1. *Etape d'engagement*: le démonstrateur choisit aléatoirement un entier r , calcule "l'engagement" $R = r^2 \bmod n$, et envoie l'engagement au
5 contrôleur;
2. *Etape de défi*: le contrôleur choisit aléatoirement m défis d_1, d_2, \dots, d_m , où d_i est égal à 0 ou 1 pour $i = 1, \dots, m$, et envoie ces défis au démonstrateur;
3. *Etape de réponse*: le démonstrateur calcule la réponse
10 $D = r \times Q_1^{d_1} \times Q_2^{d_2} \times \dots \times Q_m^{d_m} \bmod n$,
et envoie cette réponse au contrôleur; et
4. *Etape de vérification*: le contrôleur calcule
$$\left(\frac{D^2}{G_1^{d_1} \times G_2^{d_2} \times \dots \times G_m^{d_m}} \right) \bmod n$$
, et vérifie que le résultat est bien égal à
l'engagement R .

15 Cette variante "en parallèle" permet d'accélérer la procédure d'authentification de Fiat-Shamir par rapport à la variante "en série" mentionnée ci-dessus.

On notera d'ailleurs que les calculs requis pour mettre en œuvre l'une ou l'autre de ces variantes peuvent être réduits si le démonstrateur
20 utilise le "théorème des restes chinois" (bien connu des experts en théorie des nombres). Il peut opérer de la manière suivante.

Considérons tout d'abord le calcul de l'engagement R . Pour un module $n = p_1 \times p_2$, où $p_1 < p_2$, soit C le nombre positif inférieur à p_1 tel que p_1 divise $(p_2 \times C - 1)$ (ce nombre C est connu sous le nom de "reste
25 chinois"). Le démonstrateur choisit aléatoirement deux entiers r_1 et r_2 tels que $0 < r_1 < p_1$ et $0 < r_2 < p_2$, et calcule les deux "composantes d'engagement" $R_1 = r_1^2 \bmod p_1$ et $R_2 = r_2^2 \bmod p_2$. La valeur de l'engagement s'en déduit selon:

$$R = z \times p_2 + R_2, \text{ où } z = C \times (R_1 - R_2).$$

30 Ensuite, concernant le calcul de la réponse D , le démonstrateur peut opérer de la manière suivante. Définissons, pour $i = 1, \dots, m$, des "composantes de clés privées" $Q_{i,1} = Q_i \bmod p_1$ et $Q_{i,2} = Q_i \bmod p_2$. Le démonstrateur calcule d'abord les deux "composantes de réponse"

$$D_1 = r_1 \times Q_{1,1}^{d_1} \times Q_{2,1}^{d_2} \times \dots \times Q_{m,1}^{d_m} \bmod p_1, \text{ et}$$

$$35 \quad D_2 = r_2 \times Q_{1,2}^{d_1} \times Q_{2,2}^{d_2} \times \dots \times Q_{m,2}^{d_m} \bmod p_2.$$

Il obtient ensuite la valeur de la réponse selon:

$$D = z \times p_2 + D_2, \text{ où } z = C \times (D_1 - D_2).$$

L'avantage de cette méthode de calcul "à la chinoise" est que le démonstrateur calcule modulo p_1 et modulo p_2 au lieu de modulo n , dans des conditions où les nombres p_1 et p_2 sont généralement beaucoup plus petits que n .

La procédure d'authentification d'entités de Fiat-Shamir peut être aisément transposée à la vérification par un contrôleur qu'un message M qu'il a reçu lui a bien été envoyé par un certain détenteur de clés, appelé ici aussi "démonstrateur". Cette procédure d'authentification de messages comprend les étapes interactives suivantes:

1. *Etape d'engagement*: le démonstrateur choisit aléatoirement un entier r , et calcule d'abord l'engagement $R = r^2 \bmod n$, puis le "titre" (également appelé le "jeton") $T = h(M, R)$, où h est une fonction de hachage (par exemple l'une des fonctions définies dans la norme ISO/IEC 10118-3), et enfin envoie ce titre T au contrôleur;
2. *Etape de défi*: le contrôleur choisit aléatoirement un défi d , qui peut prendre la valeur 0 ou la valeur 1, et envoie ce défi au démonstrateur;
3. *Etape de réponse*: le démonstrateur calcule la réponse $D = r \times Q^d \bmod n$, et envoie cette réponse au contrôleur; et
4. *Etape de vérification*: le contrôleur calcule $h\left(M, \left(\frac{D^2}{G^d}\right) \bmod n\right)$, et vérifie que le résultat est bien égal au titre T .

On peut enfin transposer la procédure d'authentification d'entités de Fiat-Shamir de manière à définir une procédure de signature d'un message M qui est envoyé à un contrôleur par un certain détenteur de clés, appelé ici "signataire"; on notera qu'une procédure de signature n'est, quant à elle, pas interactive. Le signataire détient une pluralité de clés privées Q_1, Q_2, \dots, Q_m , où m est grand par rapport à 1, et a publié, outre un module RSA n , des clés publiques respectives G_1, G_2, \dots, G_m , où $G_i = Q_i^2 \bmod n$ pour $i = 1, \dots, m$. Cette procédure de signature comprend les étapes suivantes (auxquelles on a donné respectivement les mêmes noms que ci-dessus par analogie):

1. *Etape d'engagement*: le signataire choisit aléatoirement m entiers r_i , où $i = 1, \dots, m$, et calcule d'abord les engagements $R_i = r_i^2 \bmod n$, puis le titre $T = h(M, R_1, R_2, \dots, R_m)$, où h est une fonction de hachage produisant un mot de m bits, et enfin envoie ce titre T au contrôleur;
2. *Etape de défi*: le signataire identifie lui-même les bits d_1, d_2, \dots, d_m du titre T ;

3. *Etape de réponse*: le signataire calcule les "réponses"
 $D_i = r_i \times Q_i^{d_i} \bmod n$, et envoie ces réponses au contrôleur; et

4. *Etape de vérification*: le contrôleur calcule

$$h\left(M, \left(\frac{D_1^2}{G_1^{d_1}}\right) \bmod n, \left(\frac{D_2^2}{G_2^{d_2}}\right) \bmod n, \dots, \left(\frac{D_m^2}{G_m^{d_m}}\right) \bmod n\right),$$

5 et vérifie que le résultat est bien égal au titre T .

Examinons à présent de plus près la question de la sécurité du procédé de Fiat-Shamir. Par exemple, concernant la procédure d'authentification d'entité succinctement exposée ci-dessus, est-il possible pour un imposteur (c'est-à-dire une entité connaissant le module RSA n et la clé publique G , mais ne connaissant pas la clé privée Q de l'entité qu'elle prétend être) de tromper le contrôleur?

On notera tout d'abord que le défi, bien qu'aléatoire, ne peut prendre que deux valeurs; si un imposteur devine correctement (avec, donc, 50% de chances de succès) la valeur du défi qui lui sera, au cours de la procédure d'authentification, jeté par le contrôleur, pourra-t-il satisfaire à toutes les étapes du procédé de Fiat-Shamir sans se faire "prendre" par le contrôleur? La réponse à cette question est oui. En effet:

- si l'imposteur devine que le défi sera $d=0$, alors il fournit au contrôleur un engagement $R = r^2 \bmod n$, et une réponse $D = r$; et
- si l'imposteur devine que le défi sera $d=1$, alors il choisit un entier $l > 0$ quelconque, et fournit au contrôleur un engagement $R = l^2 \times G \bmod n$, et une réponse $D = l \times G \bmod n$.

La procédure de Fiat-Shamir présente donc une faiblesse, dont l'effet peut toutefois être atténué, comme indiqué ci-dessus, si l'on répète cette procédure en série, de manière à rendre aussi peu probable que possible une série correcte d'anticipations du défi par un imposteur éventuel. Il en résulte que, pour rendre cette procédure d'authentification suffisamment sûre, on doit en augmenter considérablement la durée.

La demande internationale WO-00/45550 divulgue un procédé de cryptographie (applicable à une procédure d'authentification d'entité, à une procédure d'authentification de message et à une procédure de signature de message) ne souffrant pas de cet inconvénient. Selon ce procédé, le démonstrateur publie non seulement un module RSA n et une clé publique G , mais également un entier (appelé "l'exposant") $v = 2^k$, où k (appelé "paramètre de sécurité") est un entier supérieur à 1. De plus,

$$G = Q^v \bmod n, \tag{1}$$

où Q est la clé privée du démonstrateur.

La procédure d'authentification selon la demande WO-00/45550 comprend les étapes suivantes:

1. *Etape d'engagement*: le démonstrateur choisit aléatoirement un entier r , calcule "l'engagement" $R = r^v \bmod n$, et envoie l'engagement au contrôleur;
- 5 2. *Etape de défi*: le contrôleur choisit aléatoirement un entier d appelé "défi", où $0 \leq d \leq 2^{k-1} - 1$, et envoie ce défi au démonstrateur;
3. *Etape de réponse*: le démonstrateur calcule la "réponse" $D = r \times Q^d \bmod n$, et envoie cette réponse au contrôleur; et
4. *Etape de vérification*: le contrôleur calcule $\left(\frac{D^v}{G^d}\right) \bmod n$, et vérifie que le résultat est bien égal à l'engagement R .

10 On voit donc que dans cette procédure le défi peut prendre 2^{k-1} valeurs différentes (au lieu de 2 valeurs seulement selon le procédé de Fiat-Shamir), ce qui rend une anticipation correcte du défi par un imposteur d'autant plus improbable que l'on choisit k grand, et cela pour une seule mise en œuvre de la succession d'étapes ci-dessus.

15 Cela étant, on peut bien sûr répéter cette procédure s fois en série et/ou utiliser m couples de clés en parallèle, comme expliqué ci-dessus, afin de renforcer la sécurité; il est alors avantageux de calculer "à la chinoise". En pratique, il est conseillé de prendre, pour le produit $[(k-1) \times m \times s]$, une valeur au moins égale à 40 en authentification et à 80 en signature (compte

20 tenu de ce qu'un attaquant dispose de plus de temps pour "craquer" le code en signature qu'en authentification).

De plus, selon la demande WO-00/45550, on requiert que la clé publique vérifie la relation

$$G = g^2 \bmod n, \quad (2)$$

25 où g est un petit entier supérieur à 1 (appelé "nombre de base"). On voit en effet, en combinant les équations (1) et (2) ci-dessus, qu'il faut trouver un couple (g, Q) satisfaisant à l'équation

$$Q^v = g^2 \bmod n, \quad (3)$$

30 pour n et v donnés; or on peut démontrer que la solution de cette équation (3) n'est possible (en un temps raisonnable) que pour quelqu'un qui connaît la factorisation du module, c'est-à-dire pour le détenteur des clés. Autrement dit, il est aussi complexe de calculer une paire de clés conforme à la demande WO-00/45550 à partir des paramètres publics correspondants, que de factoriser ce nombre n ; on dit que les deux tâches sont

35 "équivalentes" en termes de complexité, et qu'un jeu de clés impliquant une telle équivalence satisfait au "critère d'équivalence".

Un premier avantage de cet état de choses est que l'on dispose ainsi d'un niveau de sécurité de référence (à savoir le problème de la factorisation). Un second avantage est qu'il n'est pas nécessaire, pour un

détenteur de clés selon la demande WO-00/45550, de faire certifier sa clé publique par une autorité de certification, c'est-à-dire d'obtenir de cette autorité un certificat liant cette clé publique à l'identité de son détenteur; il est seulement nécessaire de faire certifier le module RSA n , les autres
 5 paramètres étant directement publiés par le détenteur lui-même. En revanche, dans le procédé de Fiat-Shamir par exemple, il est possible pour différentes entités de construire leur propre paire de clés à partir d'un même module RSA (les paires de Fiat-Shamir ne satisfont donc pas au critère d'équivalence défini ci-dessus), et par conséquent chaque clé publique
 10 particulière doit être liée par une autorité de certification à l'identité de son détenteur.

Toutefois, on peut montrer qu'il n'existe de solutions à l'équation (3) que pour certains modules n particuliers (représentant environ un quart de tous les modules RSA). Or cela est gênant pour une entité souhaitant
 15 produire des paires de clés selon la demande WO-00/45550: si cette entité possède déjà une collection de modules RSA, elle ne pourra généralement utiliser qu'une partie d'entre eux pour construire ces clés, et si elle ne possède pas déjà de modules RSA, elle aura plus de mal à trouver des modules adéquats que si tous (ou presque tous) les modules RSA étaient
 20 compatibles avec le procédé.

La présente invention concerne donc, selon un premier aspect, un procédé de cryptographie à clés asymétriques mettant en jeu un détenteur de clés possédant un nombre $m \geq 1$ de clés privées Q_1, Q_2, \dots, Q_m et de clés publiques respectives G_1, G_2, \dots, G_m , chaque paire de clés (Q_i, G_i) (où
 25 $i = 1, \dots, m$) vérifiant soit la relation $G_i = Q_i^v \bmod n$, soit la relation $G_i \times Q_i^v = 1 \bmod n$, où n est un entier public égal au produit de f facteurs premiers privés (où $f > 1$), notés p_1, \dots, p_f , dont deux au moins sont distincts, et l'exposant v est un entier public égal à une puissance de 2. Ce procédé est remarquable en ce que

$$30 \quad v = 2^{b+k},$$

où k est un entier strictement positif et $b = \max(b_1, \dots, b_f)$, où b_j (où $j = 1, \dots, f$) est le plus grand entier tel que $(p_j - 1) / 2^{b_j - 1}$ soit pair,

et en ce que chaque clé publique G_i (où $i = 1, \dots, m$) est de la forme

$$G_i = g_i^{2^{a_i}} \bmod n,$$

35 où les nombres g_i , appelés "nombres de base", sont des entiers strictement supérieurs à 1, et où les nombres a_i sont des entiers tels que $1 \leq a_i \leq b$ et tels que l'un d'entre eux au moins est strictement supérieur à 1.

On notera que la présente invention se distingue de la demande WO-00/45550 en particulier en ce que chaque clé publique est ici de la

forme $G_i = g_i^{2^{a_i}} \bmod n$, où l'un au moins des nombres a_i est strictement supérieur à 1, au lieu de $G_i = g_i^2 \bmod n$.

On montrera dans la description détaillée ci-dessous que, grâce à ces dispositions, il existe nécessairement des clés selon l'invention, c'est-à-dire des couples (g, Q) satisfaisant aux conditions succinctement exposées ci-dessus, et ce, quelle que soit la valeur choisie pour le module n , à de très rares exceptions près (ces modules particuliers n'étant en pratique jamais choisis pour mettre en œuvre le procédé RSA). Autrement dit, n'importe quel module RSA est compatible avec le procédé selon la présente invention.

Selon des caractéristiques particulières, l'un au moins desdits facteurs premiers p_1, \dots, p_f est congru à 1 modulo 4, et les entiers a_i (où $i = 1, \dots, m$) sont tous égaux audit nombre b .

Grâce à ces dispositions, la construction de jeux de clés selon l'invention est considérablement facilitée.

Selon d'autres caractéristiques particulières, il existe au moins un nombre g_s , parmi lesdits nombres de base g_1, \dots, g_m , et deux nombres p_t et p_u différents de 2 parmi lesdits facteurs premiers p_1, \dots, p_f , tels que, compte tenu desdits nombres b_1, \dots, b_f ,

- si $b_t = b_u$, alors $(g_s | p_t) = - (g_s | p_u)$, et

- si $b_t < b_u$, alors $(g_s | p_u) = -1$,

où $(g_s | p_t)$ et $(g_s | p_u)$ désignent les symboles de Legendre de g_s par rapport à p_t et p_u (la définition des "symboles de Legendre" sera rappelée dans la description détaillée ci-dessous).

On peut montrer que, grâce à ces dispositions, les clés obtenues satisfont au "critère d'équivalence" défini ci-dessus.

Selon encore d'autres caractéristiques particulières, ledit procédé met en présence un contrôleur et ledit détenteur de clés, appelé ici "démonstrateur". Ce procédé est remarquable en ce qu'il comprend les étapes suivantes:

- le démonstrateur choisit aléatoirement un entier r , calcule "l'engagement" $R = r^v \bmod n$, et envoie l'engagement au contrôleur,

- le contrôleur choisit aléatoirement m "défis" d_1, d_2, \dots, d_m , où $i = 1, \dots, m$, et envoie ces défis au démonstrateur,

- le démonstrateur calcule la "réponse"

$D = r \times Q_1^{d_1} \times Q_2^{d_2} \times \dots \times Q_m^{d_m} \bmod n$,

et envoie cette réponse au contrôleur, et

- le contrôleur calcule

$$D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times \dots \times G_m^{\varepsilon_m d_m} \bmod n$$

où, pour $i=1, \dots, m$, $\varepsilon_i = +1$ dans le cas où $G_i \times Q_i^v = 1 \bmod n$ et $\varepsilon_i = -1$ dans le cas où $G_i = Q_i^v \bmod n$,

5 et vérifie que le résultat est bien égal à l'engagement R .

Il importe de noter qu'il n'est pas nécessaire pour un contrôleur et un démonstrateur qui mettent en œuvre ce procédé d'échanger *l'intégralité* de l'engagement ou de la réponse: en effet, il leur est possible, par convention mutuelle, de n'échanger qu'une partie de ces données, ou encore le résultat
10 du hachage de tout ou partie de ces données par une fonction de hachage prédéterminée.

Naturellement, on peut avantageusement accélérer la mise en œuvre du procédé en calculant "à la chinoise".

Par exemple, concernant le calcul de l'engagement R , le
15 démonstrateur peut opérer de la manière suivante. Pour un module $n = p_1 \times p_2$, où $p_1 < p_2$, soit C le nombre positif inférieur à p_1 tel que p_1 divise $(p_2 \times C - 1)$ (ce nombre C est connu sous le nom de "reste chinois"). Le démonstrateur choisit aléatoirement deux entiers r_1 et r_2 tels que $0 < r_1 < p_1$ et $0 < r_2 < p_2$, et calcule les deux "composantes d'engagement"
20 $R_1 = r_1^v \bmod p_1$ et $R_2 = r_2^v \bmod p_2$. La valeur de l'engagement s'en déduit selon:

$$R = z \times p_2 + R_2, \text{ où } z = C \times (R_1 - R_2).$$

Le démonstrateur peut également calculer "à la chinoise" pour obtenir la réponse D , de manière analogue à la méthode de calcul décrite
25 ci-dessus pour le procédé de Fiat-Shamir.

Enfin, on notera que l'on peut se limiter à des défis vérifiant $0 \leq d_i \leq 2^k - 1$ pour $i=1, \dots, m$ (ce qui a l'avantage de simplifier les calculs aussi bien pour le démonstrateur que pour le contrôleur). En effet, on vérifie facilement que, pour deux valeurs de d_i différant de 2^k , les valeurs de $Q_i^{d_i}$
30 correspondantes se déduisent l'une de l'autre par un facteur g_i . Comme la publication des clés publiques G_i implique essentiellement la divulgation des nombres de base g_i , on voit que l'on assure le même niveau de sécurité avec des valeurs de défis situées dans l'intervalle $0 \leq d_i \leq 2^k - 1$, qu'avec des valeurs de défis sortant de cet intervalle.

35 Selon encore d'autres caractéristiques particulières, ledit procédé permet à un contrôleur de vérifier qu'un message M qu'il a reçu lui a bien été envoyé par ledit détenteur de clés, appelé ici aussi "démonstrateur". Ce procédé est remarquable en ce qu'il comprend les étapes suivantes:

- le démonstrateur choisit aléatoirement un entier r , et calcule d'abord "l'engagement" $R = r^v \bmod n$, puis le "titre" $T = h(M, R)$, où h est une fonction de hachage, et enfin envoie ce titre T au contrôleur,

5 - le contrôleur choisit aléatoirement m "défis" d_1, d_2, \dots, d_m , où $i = 1, \dots, m$, et envoie ces défis au démonstrateur,

- le démonstrateur calcule la "réponse"

$$D = r \times Q_1^{d_1} \times Q_2^{d_2} \times \dots \times Q_m^{d_m} \bmod n,$$

et envoie cette réponse au contrôleur, et

- le contrôleur calcule

10
$$h(M, D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times \dots \times G_m^{\varepsilon_m d_m} \bmod n)$$

où, pour $i = 1, \dots, m$, $\varepsilon_i = +1$ dans le cas où $G_i \times Q_i^v = 1 \bmod n$ et $\varepsilon_i = -1$ dans le cas où $G_i = Q_i^v \bmod n$,

et vérifie que le résultat est bien égal au titre T .

15 La remarque faite ci-dessus concernant les valeurs des défis dans le procédé d'authentification d'entités s'applique évidemment aussi à ce procédé d'authentification de message.

On notera également que cette procédure d'authentification de message est parfois considérée comme une forme de signature du message.

20 Selon encore d'autres caractéristiques particulières, on peut mettre en œuvre une autre façon de signer un message. Ce mode de réalisation, qui permet en effet audit détenteur de clés, appelé ici "signataire", de signer un message M qu'il envoie à un contrôleur, est remarquable en ce qu'il comprend les étapes suivantes:

25 - le signataire choisit aléatoirement m entiers r_i , où $i = 1, \dots, m$, et calcule d'abord les engagements $R = r^v \bmod n$, puis le titre $T = h(M, R_1, R_2, \dots, R_m)$, où h est une fonction de hachage produisant un mot de m bits, et enfin envoie ce titre T au contrôleur,

- le signataire identifie lui-même les bits d_1, d_2, \dots, d_m du titre T ,

30 - le signataire calcule les "réponses" $D_i = r_i \times Q_i^{d_i} \bmod n$, et envoie ces réponses au contrôleur, et

- le contrôleur calcule

$$h(M, D_1^v \times G_1^{\varepsilon_1 d_1} \bmod n, D_2^v \times G_2^{\varepsilon_2 d_2} \bmod n, \dots, D_m^v \times G_m^{\varepsilon_m d_m} \bmod n)$$

où, pour $i = 1, \dots, m$, $\varepsilon_i = +1$ dans le cas où $G_i \times Q_i^v = 1 \bmod n$ et $\varepsilon_i = -1$ dans le cas où $G_i = Q_i^v \bmod n$,

et vérifie que le résultat est bien égal au titre T .

Selon un deuxième aspect, l'invention concerne divers dispositifs.

5 Elle concerne ainsi, premièrement, un circuit électronique contenant un processeur et des mémoires. Ce circuit électronique est remarquable en qu'il peut être programmé pour mettre en œuvre, en tant que ledit détenteur de clés, l'un quelconque des procédés de cryptographie succinctement exposés ci-dessus.

10 L'invention concerne aussi, deuxièmement, un circuit électronique dédié. Ce circuit électronique est remarquable en qu'il contient des microcomposants lui permettant de traiter des données de manière à mettre en œuvre, en tant que ledit détenteur de clés, l'un quelconque des procédés de cryptographie succinctement exposés ci-dessus. Il peut en particulier
15 s'agir d'un circuit intégré (en anglais, "*Application Specific Integrated Circuit*" ou "ASIC").

Ces deux circuits électroniques peuvent par exemple se présenter sous la forme d'une "puce électronique".

20 L'invention concerne aussi, troisièmement, un objet portable destiné à être connecté à un terminal pour échanger des données avec ce terminal. Cet objet portable est remarquable en ce qu'il contient un circuit électronique tel que décrit succinctement ci-dessus, et en ce qu'il est apte à stocker des données d'identification et des clés privées propres audit détenteur de clés.

25 Cet objet portable peut par exemple être une carte à puce, ou une clé USB.

L'invention concerne aussi, quatrièmement, un terminal apte à être connecté à un objet portable pour échanger des données avec cet objet portable. Ce terminal est remarquable en ce qu'il comporte un dispositif de traitement de données programmé pour mettre en œuvre, en tant que ledit
30 contrôleur, l'un quelconque des procédés de cryptographie succinctement exposés ci-dessus.

L'invention concerne aussi, cinquièmement, un système de cryptographie comprenant un objet portable et un terminal tels que décrits succinctement ci-dessus.

35 L'invention concerne aussi, sixièmement, un moyen de stockage de données inamovible comportant des instructions de code de programme informatique pour l'exécution, en tant que ledit détenteur de clés, des étapes de l'un quelconque des procédés de cryptographie succinctement exposés ci-dessus.

40 L'invention concerne aussi, septièmement, un moyen de stockage de données partiellement ou totalement amovible, comportant des instructions de code de programme informatique pour l'exécution, en tant

que ledit détenteur de clés, des étapes de l'un quelconque des procédés de cryptographie succinctement exposés ci-dessus.

5 L'invention concerne aussi, huitièmement, un dispositif de traitement de données comprenant un moyen de stockage "détenteur de clés" tel que décrit succinctement ci-dessus.

Ce dispositif de traitement de données peut par exemple être un ordinateur personnel ou un serveur.

10 L'invention concerne aussi, neuvièmement, un moyen de stockage de données inamovible comportant des instructions de code de programme informatique pour l'exécution, en tant que ledit contrôleur, des étapes de l'un quelconque des procédés de cryptographie succinctement exposés ci-dessus.

15 L'invention concerne aussi, dixièmement, un moyen de stockage de données partiellement ou totalement amovible, comportant des instructions de code de programme informatique pour l'exécution, en tant que ledit contrôleur, des étapes de l'un quelconque des procédés de cryptographie succinctement exposés ci-dessus.

20 L'invention concerne aussi, onzièmement, un dispositif de traitement de données comprenant un moyen de stockage "contrôleur" tel que décrit succinctement ci-dessus.

Ce dispositif de traitement de données peut par exemple être un ordinateur personnel ou un serveur.

25 L'invention concerne aussi, douzièmement, un système de cryptographie comprenant un dispositif de traitement de données "détenteur de clés" et un dispositif de traitement de données "contrôleur" tels que décrits succinctement ci-dessus.

Les avantages offerts par ces dispositifs sont essentiellement les mêmes que ceux offerts par les procédés correspondants succinctement exposés ci-dessus.

30 L'invention vise également un programme d'ordinateur contenant des instructions telles que, lorsque ledit programme commande un dispositif de traitement de données programmable, lesdites instructions font que ledit dispositif de traitement de données met en œuvre l'un des procédés de cryptographie succinctement exposés ci-dessus.

35 Les avantages offerts par ce programme d'ordinateur sont essentiellement les mêmes que ceux offerts par les procédés de cryptographie succinctement exposés ci-dessus.

D'autres aspects et avantages de l'invention apparaîtront à la lecture de la description détaillée ci-dessous.

40 Considérons un module, noté n , qui est en général le produit de f grands facteurs premiers (où $f > 1$), notés p_1, \dots, p_f , dont deux au moins sont distincts:

$$n = p_1 \times \dots \times p_f, \text{ où } p_1 \leq \dots \leq p_f \text{ et } p_1 < p_f.$$

A chaque facteur p_j , où $j=1, \dots, f$, on peut associer un entier strictement positif b_j défini de la manière suivante: $(p_j - 1)$ est divisible par 2^{b_j} , mais pas par 2^{b_j+1} (autrement dit, b_j est le plus grand entier tel que $(p_j - 1)/2^{b_j-1}$ soit pair). On vérifie aisément que $b_j = 1$ si $p_j = 3 \bmod 4$, et $b_j > 1$ si $p_j = 1 \bmod 4$.

Lorsqu'une entité souhaite devenir un détenteur de clés, elle peut demander à une autorité de certification de lui attribuer un module RSA n . L'entité construit alors un nombre $m \geq 1$ de clés privées Q_1, Q_2, \dots, Q_m , et publie ledit module n , un "exposant" v et des clés publiques respectives G_1, G_2, \dots, G_m .

Selon l'invention, ces diverses quantités obéissent aux conditions suivantes:

- l'exposant est de la forme

$$v = 2^{b+k},$$

où $b = \max(b_1, \dots, b_f)$ et $k \geq 1$,

- chaque clé publique G_i (où $i = 1, \dots, m$) est de la forme

$$G_i = g_i^{2^{a_i}} \bmod n,$$

où les nombres g_i (appelés "nombres de base") sont des entiers strictement supérieurs à 1, et où les nombres a_i sont des entiers tels que $1 \leq a_i \leq b$ et tels que l'un d'entre eux au moins est strictement supérieur à 1, et

- chaque paire de clés (Q_i, G_i) (où $i = 1, \dots, m$) vérifie

$$\bullet \text{ soit la relation } G_i = Q_i^v \bmod n, \quad (1i)$$

$$\bullet \text{ soit la relation } G_i \times Q_i^v = 1 \bmod n. \quad (1'i)$$

On peut montrer que, pour que des paires de clés satisfaisant à ces conditions puissent exister, il faut que le rang de chaque clé G_i par rapport à chaque facteur premier p_j soit impair. On rappelle à cet égard que "le rang λ par rapport à p " d'un élément x non-nul du corps des entiers modulo p (où p est premier) est le plus petit entier λ strictement positif tel que $x^\lambda = 1 \bmod p$ (où les puissances successives de x sont prises modulo p).

La condition selon laquelle le rang de G_i par rapport à chacun des facteurs premiers du module n est impair implique qu'aucun facteur premier

p_j ne peut être tel que $(p_j - 1)$ soit égal à une puissance de 2; mais les nombres premiers vérifiant cette condition (par exemple 3, 5, 17, ou 257) sont rares, et même très rares si l'on choisit des grands nombres pour les facteurs premiers du module.

- 5 Cette propriété des clés publiques peut être obtenue en choisissant les entiers g_i et a_i conformément à la règle suivante:

$$a_i \geq h(g_i) \bmod p_j \text{ pour tout } j = 1, \dots, f,$$

- 10 où, pour tout entier x non-nul du corps des entiers modulo p (où p est premier), on définit la "hauteur de x par rapport à p ", notée $h(x) \bmod p$, comme étant la plus grande puissance de 2 qui divise le rang de x par rapport à p .

On va maintenant présenter, à titre d'exemple non limitatif, un mode de réalisation particulier.

- 15 Selon ce mode de réalisation, on choisit les facteurs premiers p_j du module n de telle sorte que l'un au moins d'entre eux soit congru à 1 modulo 4 (les autres facteurs pouvant être congrus soit à 1, soit à 3 modulo 4). Il résulte des propriétés des nombres b_j associés énoncées ci-dessus que:

$$b > 1.$$

De plus, on prend

- 20 $G_i = g_i^{2^b} \bmod n$, pour tout $i = 1, \dots, m$. (4)

On notera que, par contraste, les clés définies dans la demande WO-00/45550 (vérifiant, comme indiqué ci-dessus, $Q_i^v = g_i^2 \bmod n$) n'existent que pour les modules dont *tous* les facteurs premiers sont congrus à 3 modulo 4.

- 25 On peut montrer que les clés publiques G_i définies par l'équation (4) sont de rang impair par rapport à chacun des facteurs premiers du module.

Enfin, on requiert qu'il existe au moins un nombre g_s , parmi lesdits nombres de base g_1, \dots, g_m , et deux nombres p_t et p_u différents de 2 parmi lesdits facteurs premiers p_1, \dots, p_f , tels que

- 30 - si $b_t = b_u$, alors $(g_s | p_t) = -(g_s | p_u)$, et (5a)

$$- \text{si } b_t < b_u, \text{ alors } (g_s | p_u) = -1, \quad (5b)$$

où les nombres b_t et b_u (voir définition ci-dessus) sont déterminés par rapport à p_t et p_u , et $(g_s | p_t)$ et $(g_s | p_u)$ désignent les symboles de Legendre de g_s correspondants.

On rappelle à cet égard que le "symbole de Legendre par rapport à p ", noté ici $(x|p)$, d'un élément x non-nul du corps des entiers modulo p (où p est un nombre premier différent de 2) est égal à $x^{(p-1)/2} \bmod p$. On montre facilement que $(x|p)=0$ si x est un multiple de p , $(x|p)=+1$ si x est égal au carré modulo p d'un autre élément du corps, et $(x|p)=-1$ sinon.

Le mode de réalisation des équations (5a-5b) représente un exemple de mise en œuvre de l'invention où les clés satisfont au "critère d'équivalence", c'est-à-dire qu'il est impossible, à partir des paramètres publics n , v et G_1, G_2, \dots, G_m , de calculer (en un temps raisonnable) les clés privées Q_1, Q_2, \dots, Q_m , à moins de connaître les facteurs premiers du module.

En revanche, si l'on connaît la factorisation du module, on peut obtenir les clés privées de la façon suivante. Soit A le plus petit commun multiple des nombres $(p_j-1)/2^b$, où $j=1, \dots, f$, et soit u le plus petit entier positif tel que $(u \times v + 1)$ soit un multiple de A . Chaque clé privée vérifie:

$$Q_i \times G_i^u = 1 \bmod n \quad \text{si l'on a choisi l'équation (1'i) (soit } G_i = Q_i^v \bmod n), \text{ ou}$$

$$Q_i = G_i^u \bmod n \quad \text{si l'on a choisi l'équation (1'i) (soit } G_i \times Q_i^v = 1 \bmod n).$$

On peut également calculer les clés privées Q_1, Q_2, \dots, Q_m , au moyens de calculs "à la chinoise".

On terminera par quelques remarques concernant les nombres de base.

Il a été constaté que les calculs effectués durant la mise en œuvre du procédé selon l'invention sont d'autant plus rapides que les nombres de base sont faibles. Il est donc conseillé de les choisir aussi petits que possible.

Par exemple, on peut choisir les nombres de base parmi les 54 premiers nombres premiers (le cinquante-quatrième nombre premier étant 251).

En variante, on peut prendre systématiquement les m premiers nombres premiers comme nombres de base, c'est-à-dire, $g_1=2$, $g_2=3$, $g_3=5$, $g_4=7$, $g_5=11$, et ainsi de suite. Cette approche a l'avantage de la simplicité, mais elle ne garantit pas que l'on obtienne un jeu de clés satisfaisant au critère d'équivalence. Cependant, on peut montrer que la proportion de jeux ne satisfaisant pas au critère d'équivalence est inférieure à $1/2^m$; par exemple, pour $m=16$ (correspondant à $g_{16}=53$), cette proportion vaut moins de $1/65\,536$.

REVENDICATIONS

1. Procédé de cryptographie à clés asymétriques mettant en jeu un détenteur de clés possédant un nombre $m \geq 1$ de clés privées Q_1, Q_2, \dots, Q_m et de clés publiques respectives G_1, G_2, \dots, G_m , chaque paire de clés (Q_i, G_i) (où $i = 1, \dots, m$) vérifiant soit la relation $G_i = Q_i^v \bmod n$, soit la relation $G_i \times Q_i^v = 1 \bmod n$, où n est un entier public égal au produit de f facteurs premiers privés (où $f > 1$), notés p_1, \dots, p_f , dont deux au moins sont distincts, et l'exposant v est un entier public égal à une puissance de 2, caractérisé en ce que

$$v = 2^{b+k},$$

où k est un entier strictement positif et $b = \max(b_1, \dots, b_f)$, où b_j (où $j = 1, \dots, f$) est le plus grand entier tel que $(p_j - 1) / 2^{b_j - 1}$ soit pair,

- et en ce que chaque clé publique G_i (où $i = 1, \dots, m$) est de la forme

$$G_i = g_i^{2^{a_i}} \bmod n,$$

où les nombres g_i , appelés "nombres de base", sont des entiers strictement supérieurs à 1, et où les nombres a_i sont des entiers tels que $1 \leq a_i \leq b$ et tels que l'un d'entre eux au moins est strictement supérieur à 1.

2. Procédé selon la revendication 1, caractérisé en ce que l'un au moins desdits facteurs premiers p_1, \dots, p_f est congru à 1 modulo 4, et en ce que les entiers a_i (où $i = 1, \dots, m$) sont tous égaux audit nombre b .

3. Procédé selon la revendication 1 ou la revendication 2, caractérisé en ce que il existe au moins un nombre g_s , parmi lesdits nombres de base g_1, \dots, g_m , et deux nombres p_t et p_u différents de 2 parmi lesdits facteurs premiers p_1, \dots, p_f , tels que, compte tenu desdits nombres b_1, \dots, b_f ,

- si $b_t = b_u$, alors $(g_s | p_t) = - (g_s | p_u)$, et

- si $b_t < b_u$, alors $(g_s | p_u) = -1$,

- où $(g_s | p_t)$ et $(g_s | p_u)$ désignent les symboles de Legendre de g_s par rapport à p_t et p_u .

4. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que les nombres de base g_1, \dots, g_m sont des nombres premiers.

5. Procédé selon l'une quelconque des revendications 1 à 4, dans lequel sont mis en présence un contrôleur et ledit détenteur de clés, appelé ici "démonstrateur", caractérisé en ce qu'il comprend les étapes suivantes:

- le démonstrateur choisit aléatoirement un entier r , calcule "l'engagement" $R = r^v \bmod n$, et envoie l'engagement au contrôleur,

- le contrôleur choisit aléatoirement m "défis" d_1, d_2, \dots, d_m , où $i = 1, \dots, m$, et envoie ces défis au démonstrateur,

- le démonstrateur calcule la "réponse"

$$D = r \times Q_1^{d_1} \times Q_2^{d_2} \times \dots \times Q_m^{d_m} \bmod n,$$

- 10 et envoie cette réponse au contrôleur, et

- le contrôleur calcule

$$D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times \dots \times G_m^{\varepsilon_m d_m} \bmod n$$

où, pour $i = 1, \dots, m$, $\varepsilon_i = +1$ dans le cas où $G_i \times Q_i^v = 1 \bmod n$ et $\varepsilon_i = -1$ dans le cas où $G_i = Q_i^v \bmod n$,

- 15 et vérifie que le résultat est bien égal à l'engagement R .

6. Procédé selon l'une quelconque des revendications 1 à 4, permettant à un contrôleur de vérifier qu'un message M qu'il a reçu lui a bien été envoyé par ledit détenteur de clés, appelé ici "démonstrateur", caractérisé en ce qu'il comprend les étapes suivantes:

- 20 - le démonstrateur choisit aléatoirement un entier r , et calcule d'abord "l'engagement" $R = r^v \bmod n$, puis le "titre" $T = h(M, R)$, où h est une fonction de hachage, et enfin envoie ce titre T au contrôleur,

- le contrôleur choisit aléatoirement m "défis" d_1, d_2, \dots, d_m , où $i = 1, \dots, m$, et envoie ces défis au démonstrateur,

- 25 - le démonstrateur calcule la "réponse"

$$D = r \times Q_1^{d_1} \times Q_2^{d_2} \times \dots \times Q_m^{d_m} \bmod n,$$

et envoie cette réponse au contrôleur, et

- le contrôleur calcule

$$h\left(M, D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times \dots \times G_m^{\varepsilon_m d_m} \bmod n\right)$$

- 30 où, pour $i = 1, \dots, m$, $\varepsilon_i = +1$ dans le cas où $G_i \times Q_i^v = 1 \bmod n$ et $\varepsilon_i = -1$ dans le cas où $G_i = Q_i^v \bmod n$,

et vérifie que le résultat est bien égal au titre T .

7. Procédé selon la revendication 5 ou la revendication 6, caractérisé en ce que les défis vérifient $0 \leq d_i \leq 2^k - 1$ pour $i = 1, \dots, m$.

8. Procédé selon l'une quelconque des revendications 1 à 4, permettant audit détenteur de clés, appelé ici "signataire", de signer un message M qu'il envoie à un contrôleur, caractérisé en ce qu'il comprend les étapes suivantes:

- le signataire choisit aléatoirement m entiers r_i , où $i = 1, \dots, m$, et calcule d'abord les engagements $R = r^v \bmod n$, puis le titre $T = h(M, R_1, R_2, \dots, R_m)$, où h est une fonction de hachage produisant un mot de m bits, et enfin envoie ce titre T au contrôleur,

- le signataire identifie lui-même les bits d_1, d_2, \dots, d_m du titre T ,

- le signataire calcule les "réponses" $D_i = r_i \times Q_i^{d_i} \bmod n$, et envoie ces réponses au contrôleur, et

- le contrôleur calcule

$$h\left(M, D_1^v \times G_1^{\varepsilon_1 d_1} \bmod n, D_2^v \times G_2^{\varepsilon_2 d_2} \bmod n, \dots, D_m^v \times G_m^{\varepsilon_m d_m} \bmod n\right)$$

où, pour $i = 1, \dots, m$, $\varepsilon_i = +1$ dans le cas où $G_i \times Q_i^v = 1 \bmod n$ et $\varepsilon_i = -1$ dans le cas où $G_i = Q_i^v \bmod n$,

et vérifie que le résultat est bien égal au titre T .

9. Circuit électronique contenant un processeur et des mémoires, caractérisé en qu'il peut être programmé pour mettre en œuvre, en tant que ledit détenteur de clés, un procédé selon l'une quelconque des revendications 1 à 8.

10. Circuit électronique dédié, caractérisé en qu'il contient des microcomposants lui permettant de traiter des données de manière à mettre en œuvre, en tant que ledit détenteur de clés, un procédé selon l'une quelconque des revendications 1 à 8.

11. Objet portable destiné à être connecté à un terminal pour échanger des données avec ce terminal, caractérisé en ce qu'il contient un circuit électronique selon la revendication 9 ou la revendication 10, et en ce qu'il est apte à stocker des données d'identification et des clés privées propres audit détenteur de clés.

12. Terminal apte à être connecté à un objet portable pour échanger des données avec cet objet portable, caractérisé en ce qu'il comporte un dispositif de traitement de données programmé pour mettre en œuvre, en tant que ledit contrôleur, un procédé selon l'une quelconque des revendications 1 à 8.

13. Système de cryptographie comprenant un objet portable selon la revendication 11 et un terminal selon la revendication 12.

14. Moyen de stockage de données inamovible comportant des instructions de code de programme informatique pour l'exécution, en tant que ledit détenteur de clés, des étapes de l'un quelconque des procédés d'un procédé selon l'une quelconque des revendications 1 à 8.
- 5 15. Moyen de stockage de données partiellement ou totalement amovible, comportant des instructions de code de programme informatique pour l'exécution, en tant que ledit détenteur de clés, des étapes d'un procédé selon l'une quelconque des revendications 1 à 8.
- 10 16. Dispositif de traitement de données comprenant un moyen de stockage selon la revendication 14 ou la revendication 15.
17. Moyen de stockage de données inamovible comportant des instructions de code de programme informatique pour l'exécution, en tant que ledit contrôleur, des étapes de l'un quelconque des procédés d'un procédé selon l'une quelconque des revendications 1 à 8.
- 15 18. Moyen de stockage de données partiellement ou totalement amovible, comportant des instructions de code de programme informatique pour l'exécution, en tant que ledit contrôleur, des étapes d'un procédé selon l'une quelconque des revendications 1 à 8.
19. Dispositif de traitement de données, caractérisé en ce qu'il comprend un moyen de stockage selon la revendication 17 ou la revendication 18.
- 20 20. Système de cryptographie comprenant un dispositif de traitement de données selon la revendication 16 et un dispositif de traitement de données selon la revendication 19.
- 25 21. Programme d'ordinateur contenant des instructions telles que, lorsque ledit programme commande un dispositif de traitement de données programmable, lesdites instructions font que ledit dispositif de traitement de données met en œuvre un procédé selon l'une quelconque des revendications 1 à 8.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2005/000158

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, INSPEC, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 00/45550 A (FRANCE TELECOM; TELEDIFFUSION DE FRANCE; MATH RIZK; GUILLOU, LOUIS; QU) 3 August 2000 (2000-08-03) cited in the application page 3, line 1 - line 27	1,9-21
A	GUILLOU L C ET AL: "Cryptographic authentication protocols for smart cards" COMPUTER NETWORKS, ELSEVIER SCIENCE PUBLISHERS B.V., AMSTERDAM, NL, vol. 36, no. 4, 16 July 2001 (2001-07-16), pages 437-451, XP004304908 ISSN: 1389-1286 page 445, right-hand column, last paragraph - page 447, left-hand column, last paragraph page 448, paragraph 3.6.2	1,9-21
	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

10 June 2005

Date of mailing of the international search report

20/06/2005

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Holper, G

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2005/000158

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>WO 02/073876 A (TELEDIFFUSION FSE ; GUILLOU LOUIS (FR); FRANCE TELECOM (FR)) 19 September 2002 (2002-09-19) page 6, line 5 - page 7, line 4 -----</p>	1,9-21

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR2005/000158

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 0045550	A	03-08-2000	FR 2788910 A1	28-07-2000
			FR 2788911 A1	28-07-2000
			FR 2788908 A1	28-07-2000
			FR 2788912 A1	28-07-2000
			FR 2824974 A1	22-11-2002
			AU 769464 B2	29-01-2004
			AU 2298400 A	25-08-2000
			AU 769444 B2	29-01-2004
			AU 2298500 A	25-08-2000
			AU 769446 B2	29-01-2004
			AU 2298600 A	18-08-2000
			CA 2360887 A1	10-08-2000
			CA 2360954 A1	03-08-2000
			CA 2361627 A1	10-08-2000
			CN 1372739 A	02-10-2002
			CN 1408154 A	02-04-2003
			CN 1468479 A	14-01-2004
			EP 1145472 A2	17-10-2001
			EP 1145473 A2	17-10-2001
			EP 1145482 A2	17-10-2001
			WO 0046946 A2	10-08-2000
			WO 0046947 A2	10-08-2000
			WO 0045550 A2	03-08-2000
			JP 2003513480 T	08-04-2003
			JP 2003519447 T	17-06-2003
			JP 2002540653 T	26-11-2002
			AU 765538 B2	18-09-2003
			AU 7669900 A	10-05-2001
			AU 766102 B2	09-10-2003
			AU 7670000 A	10-05-2001
			CA 2386748 A1	12-04-2001
			CA 2388084 A1	12-04-2001
			CN 1387714 A	25-12-2002
			CN 1433609 A	30-07-2003
			EP 1216536 A1	26-06-2002
			EP 1216537 A1	26-06-2002
			WO 0126278 A1	12-04-2001
			WO 0126279 A1	12-04-2001
			JP 2003511899 T	25-03-2003
			JP 2004527139 T	02-09-2004
WO 02073876	A	19-09-2002	FR 2822002 A1	13-09-2002
			CA 2440546 A1	19-09-2002
			CN 1504028 A	09-06-2004
			EP 1368930 A2	10-12-2003
			WO 02073876 A2	19-09-2002
			JP 2004530331 T	30-09-2004
			US 2004133781 A1	08-07-2004

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No

PCT/FR2005/000158

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

EPO-Internal, INSPEC, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>WO 00/45550 A (FRANCE TELECOM; TELEDIFFUSION DE FRANCE; MATH RIZK; GUILLOU, LOUIS; QU) 3 août 2000 (2000-08-03) cité dans la demande page 3, ligne 1 - ligne 27</p> <p>----- -/--</p>	1,9-21

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

- "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- "E" document antérieur, mais publié à la date de dépôt international ou après cette date
- "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

- "T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
- "X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- "Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
- "&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

10 juin 2005

Date d'expédition du présent rapport de recherche internationale

20/06/2005

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Holper, G

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No

PCT/FR2005/000158

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>GUILLOU L C ET AL: "Cryptographic authentication protocols for smart cards" COMPUTER NETWORKS, ELSEVIER SCIENCE PUBLISHERS B.V., AMSTERDAM, NL, vol. 36, no. 4, 16 juillet 2001 (2001-07-16), pages 437-451, XP004304908 ISSN: 1389-1286 page 445, colonne de droite, dernier alinéa - page 447, colonne de gauche, dernier alinéa page 448, alinéa 3.6.2</p>	1,9-21
A	<p>WO 02/073876 A (TELEDIFFUSION FSE ; GUILLOU LOUIS (FR); FRANCE TELECOM (FR)) 19 septembre 2002 (2002-09-19) page 6, ligne 5 - page 7, ligne 4</p>	1,9-21

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Dem. de Internationale No

PCT/FR2005/000158

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)			Date de publication
WO 0045550	A	03-08-2000	FR	2788910	A1	28-07-2000
			FR	2788911	A1	28-07-2000
			FR	2788908	A1	28-07-2000
			FR	2788912	A1	28-07-2000
			FR	2824974	A1	22-11-2002
			AU	769464	B2	29-01-2004
			AU	2298400	A	25-08-2000
			AU	769444	B2	29-01-2004
			AU	2298500	A	25-08-2000
			AU	769446	B2	29-01-2004
			AU	2298600	A	18-08-2000
			CA	2360887	A1	10-08-2000
			CA	2360954	A1	03-08-2000
			CA	2361627	A1	10-08-2000
			CN	1372739	A	02-10-2002
			CN	1408154	A	02-04-2003
			CN	1468479	A	14-01-2004
			EP	1145472	A2	17-10-2001
			EP	1145473	A2	17-10-2001
			EP	1145482	A2	17-10-2001
			WO	0046946	A2	10-08-2000
			WO	0046947	A2	10-08-2000
			WO	0045550	A2	03-08-2000
			JP	2003513480	T	08-04-2003
			JP	2003519447	T	17-06-2003
			JP	2002540653	T	26-11-2002
			AU	765538	B2	18-09-2003
			AU	7669900	A	10-05-2001
			AU	766102	B2	09-10-2003
			AU	7670000	A	10-05-2001
			CA	2386748	A1	12-04-2001
			CA	2388084	A1	12-04-2001
			CN	1387714	A	25-12-2002
			CN	1433609	A	30-07-2003
			EP	1216536	A1	26-06-2002
			EP	1216537	A1	26-06-2002
			WO	0126278	A1	12-04-2001
			WO	0126279	A1	12-04-2001
			JP	2003511899	T	25-03-2003
			JP	2004527139	T	02-09-2004
WO 02073876	A	19-09-2002	FR	2822002	A1	13-09-2002
			CA	2440546	A1	19-09-2002
			CN	1504028	A	09-06-2004
			EP	1368930	A2	10-12-2003
			WO	02073876	A2	19-09-2002
			JP	2004530331	T	30-09-2004
			US	2004133781	A1	08-07-2004